

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 Residence Located at  
 2000 Northeast 16th Street, Renton, Washington  
 More Fully Described in Attachment A

Case No. MJ21-309

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A Residence, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

## Offense Description

21 U.S.C. § 841(a)(1) and 846  
 21 U.S.C. § 843(b)

Distribution, Possession and Conspiracy with Intent to Distribute Controlled Substance  
 Unlawful Use of U.S. Mails to Facilitate Distribution of Controlled Substances

The application is based on these facts:

- ☒ See Affidavit of USPS Special Agent Casey Snyder, attached hereto and incorporated herein by reference.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.



CASEY J. SNYDER, Special Agent, USPS OIG

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/26/2021



Judge's signature

City and state: Seattle, Washington

BRIAN A. TSUCHIDA, United States Magistrate Judge

Printed name and title

I, Casey J. Snyder, being first duly sworn on oath, hereby depose and say:

2. **Duties, Training & Experience.** As part of my duties, I investigate the use of the U.S. mails to illegally mail and receive controlled substances, the proceeds of drug trafficking, as well as other instrumentalities associated with drug trafficking, in violation of Title 21, United States Code, Sections 841(a)(1) (distribution and possession with intent to distribute controlled substances), 843(b) (unlawful use of a communication facility, including the U.S. mails, to facilitate the distribution of controlled substances and proceeds from the sale thereof), and 846 (controlled substances conspiracy). As set forth

1 below, my training and experience includes identifying parcels with characteristics  
2 indicative of criminal activity. During my employment with the USPS-OIG, I have  
3 participated in many criminal investigations involving suspicious parcels and controlled  
4 substances.

### 5 INTRODUCTION AND PURPOSE OF AFFIDAVIT

6 3. This affidavit is submitted in support of an application for search warrants  
7 for the following location, person, and vehicle:

8 (a) 2000 Northeast 16<sup>th</sup> Street, Renton, Washington, 98056 (Herein  
9 referred to as the "**SUBJECT PREMISES**"), further described in Attachment A, which  
10 is incorporated herein by reference.

11 4. For the **SUBJECT PREMISES**, authority to search extends to all parts of  
12 the property, including main structure, garage(s), storage structures, outbuildings, and  
13 curtilage, and all vehicles, containers, compartments, or safes located on the property,  
14 whether locked or not, where the items described in Attachment B (items to be seized)  
15 could be found.

16 5. As set forth below, there is probable cause to believe that the **SUBJECT**  
17 **PREMISES**, will contain or possess evidence, fruits, and instrumentalities of possession  
18 of controlled substances with intent to distribute, and distribution of controlled  
19 substances, in violation of Title 21, United States Code, Section 841(a). I seek  
20 authorization to search and seize the items specified in Attachment B, which is  
21 incorporated herein by reference.

22 6. The information contained in this affidavit is based upon knowledge I  
23 gained from my investigation, my personal observations, my training and experience, and  
24 investigation by other law enforcement officers. Because this affidavit is being submitted  
25 for the limited purpose of securing a search warrant, I have not included every fact of  
26 which I am aware pertaining to the investigation. I have set forth only those facts that I  
27 believe are relevant to determination of probable cause to support the issuance of the  
28

1 requested warrants. When the statements of others are set forth in this affidavit, they are  
2 set forth in substance and in part.

### 3 THE INVESTIGATION

4 7. In November of 2020, investigators with the United States Postal  
5 Inspection Service (USPIS) identified multiple parcels being mailed from various  
6 locations to Bellevue, Washington. The parcel were Express Mail parcels, paid in cash,  
7 and primarily destined to the same Postal Service delivery route. The delivery route was  
8 identified as route 83, in Bellevue, Washington. Postal Service records indicated this  
9 route was normally delivered by TRI HIEN DUONG. Evidence indicates that DUONG,  
10 a Postal Service employee, is using his position with the USPS to traffic controlled  
11 substances and/or the proceeds from the sale of controlled substances. The investigation  
12 has shown DUONG is receiving parcels on his delivery route, which contain United  
13 States currency. He takes these parcels to his home address or other locations instead of  
14 delivering them.

15 8. The parcels appeared to be destined to true and deliverable addresses, but to  
16 names which did not associate to those addresses. Furthermore, the parcels are regularly  
17 mailed from the same city and state, such as Oak Grove, Kentucky; Clarksville,  
18 Tennessee; and Atlanta, Georgia. With few exceptions, the Express Mail parcels only  
19 arrive on days when DUONG is on duty and delivers mail on route 83.

20 9. Postal Service records show DUONG's address as 16004 Lake Hills  
21 Boulevard, Bellevue, Washington, 98008. Physical surveillance and law enforcement  
22 records show DUONG resides at 15103 Southeast Newport Way, Bellevue, Washington,  
23 98006. On January 13, 2021, investigators obtained a federal warrant to track DUONG's  
24 personal vehicle, a red, Acura RDX, bearing Washington license plate BWP2727 (Herein  
25 referred to as DUONG's red Acura). Data from the tracker affixed to the DUONG's red  
26 Acura, combined with physical surveillance, has confirmed DUONG's residence to be  
27 15103 Southeast Newport Way, Bellevue, Washington.  
28

1        10.        According to law enforcement records, DUONG is 33 years old, with a  
2 prior Washington State conviction for Possession of Controlled Substances with no  
3 Prescription (2019). DUONG also had an arrest in 2017 which appeared not to have led  
4 to a conviction, for Possession of a Controlled Substance with no Prescription.

5        11.        On December 11, 2020, investigators executed a federal search warrant on  
6 Express Mail parcel EJ253292487US, which was mailed from Cadiz, Kentucky to Duong  
7 T, 16004 Lake Hills Boulevard, Bellevue, Washington 98008. In obtaining probable  
8 cause to search the parcel, investigators utilized a narcotics detection canine, who alerted  
9 to the presence of controlled substances, in or on the parcel. This parcel contained  
10 \$52,000 in United States currency.

11        12.        On December 31, 2020, investigators conducted surveillance on DUONG.  
12 Postal Service records indicated two Express Mail parcels, similar to the parcels  
13 described above, were intended for DUONG's delivery route; however, they did not  
14 arrive to be delivered. Postal Service records showed DUONG, while on-duty with the  
15 Postal Service, drove to his residence at 15103 Southeast Newport Way, Bellevue,  
16 Washington. Postal Service records confirmed this address is not on the delivery route  
17 DUONG was assigned to. DUONG stayed at this location for approximately 17 minutes;  
18 before returning to his place of work; located at 13400 Southeast 30th Street, Bellevue,  
19 Washington 98005.

20        13.        On January 7, 2020, investigators conducted surveillance on DUONG as he  
21 delivered mail. Postal Service records indicated two Express Mail parcels were destined  
22 to Duong's delivery route. Both parcels were similar to the parcels described above.  
23 With the assistance of covert cameras installed in the delivery vehicle operated by  
24 DUONG, investigators observed DUONG bring two Express Mail parcels into his  
25 delivery vehicle. At approximately 11:08am, DUONG scanned both parcels as delivered.  
26 DUONG was not in the vicinity of the destination addresses when he did so. DUONG  
27 then drove, in the Postal Service delivery vehicle, to his residence, at 15103 Southeast  
28 Newport Way, Bellevue, Washington. After arriving at the **SUBJECT PREMISES**,

1 DUONG removed both parcels from the vehicle and walked towards the residence.  
2 When he returned to the vehicle, he did not have the parcels. DUONG departed the  
3 location and resumed delivering mail. When DUONG finished work, he drove his red  
4 Acura directly to his residence. Approximately 15 minutes later, DUONG departed in his  
5 red Acura and drove to 2000 Northeast 16<sup>th</sup> Street, Renton, Washington.

6 14. Law enforcement records show 2000 Northeast 16<sup>th</sup> Street, Renton,  
7 Washington is owned by TAI LING-CHEN. Law enforcement records showed a TAN  
8 VAN NGUYEN as associated with this address.

9 15. According to law enforcement records, NGUYEN is 43 years old. Law  
10 enforcement records indicated in 2004, NGUYEN was federally convicted of Conspiracy  
11 to Traffic in Marijuana. In 2005, NGUYEN was federally convicted of Conspiracy to  
12 Engage in Money Laundering. In 2013, NGUYEN was federally convicted of  
13 Conspiracy of Producing Marijuana; Specifically, Indoor Marijuana Cultivation.

14 16. On January 12, 2021, investigators conducted surveillance on DUONG.  
15 Postal Service records indicated DUONG handled/scanned two Express Mail parcels  
16 similar to those described above. Investigators followed DUONG from his delivery route  
17 to his residence at 15103 Southeast Newport Way, Bellevue, Washington. DUONG  
18 exited the delivery vehicle with what appeared to be two Express Mail parcels. DUONG  
19 appeared to enter the residence with the parcels. A few minutes later, DUONG exited the  
20 residence without the parcels, entered the delivery vehicle, and departed.

21 17. On January 15, 2021, Postal Service records indicated an Express Mail  
22 parcel similar to those described above was destined to DUONG's delivery route. Using  
23 the covert cameras in DUONG's delivery vehicle, investigators observed DUONG scan  
24 the parcel, then handle his cell phone. DUONG then removed the label from the Express  
25 Mail parcel and placed the parcel in his black backpack. After doing so, DUONG again  
26 handled his cell phone. Data from the GPS tracker affixed to DUONG's red Acura  
27 indicated DUONG drove directly from work that afternoon to the **SUBJECT**  
28 **PREMISES.**

1       18.     On January 25, 2021, Postal Service records indicated two Express Mail  
2 parcels, similar to those described above, were destined to DUONG's delivery route.  
3 One originated in Kentucky, the other in Tennessee. Using the covert cameras in  
4 DUONG's delivery vehicle, investigators were able to observe DUONG scan the parcels  
5 as delivered and remove the labels from the parcels. DUONG drove the Postal Service  
6 delivery vehicle to his residence, at 15103 Southeast Newport Way, Bellevue,  
7 Washington, and exited the vehicle. DUONG returned to the delivery vehicle and  
8 retrieved the two Express Mail parcels, then walked back to the residence. DUONG  
9 returned to the delivery vehicle without the parcels. DUONG appeared to make a phone  
10 call before driving back towards his delivery route and resuming his duties. Data from  
11 the GPS tracker affixed to DUONG's red Acura indicated he drove that night to the  
12 **SUBJECT PREMISES.**

13       19.     On February 4, 2021, investigators surveilled DUONG, with the assistance  
14 of the tracker affixed to DUONG's red Acura. Postal Service records indicated two  
15 Express Mail parcels, similar to those described above, were destined to DUONG's  
16 delivery route. Postal Service records additionally showed that DUONG handled both  
17 parcels, but due to equipment failure, investigators were not able to observe him doing  
18 so. Investigators observed DUONG leave work that afternoon and place a black  
19 backpack, similar to the black backpack used previously, in the rear of his red Acura.  
20 That evening, investigators observed DUONG drive his red Acura to the **SUBJECT**  
21 **PREMISES.** DUONG entered and exited the residence carrying what appeared to be a  
22 large dark bag or backpack which he placed in the rear of the DUONG's red Acura.  
23 DUONG then drove back to his residence at 15103 Southeast Newport Way, Bellevue,  
24 Washington.

25       20.     On February 26, 2021, Postal Service records indicated two Express Mail  
26 parcels, similar to those described above, were destined to DUONG's delivery route.  
27 One of these parcels originated in Atlanta, GA, the other in Clarksville, TN. Using the  
28 covert cameras in DUONG's delivery vehicle, investigators observed DUONG enter his

1 delivery vehicle with two Express Mail parcels which he scanned as delivered. DUONG  
2 handled his cell phone, while driving the Postal Service delivery vehicle to his residence  
3 at 15103 Southeast Newport Way, Bellevue, Washington. Upon arriving at this  
4 residence, DUONG took the two Express Mail parcels from the delivery vehicle and  
5 walked towards the residence. When DUONG returned to the delivery vehicle, he did  
6 not have the parcels. Data from the GPS tracker affixed to DUONG's red Acura showed  
7 DUONG drove home after work. After approximately three hours, DUONG departed his  
8 residence in his red Acura and drove directly to the **SUBJECT PREMISES**.

9 21. On March 9, 2021, Postal Service records indicated an Express Mail parcel,  
10 similar to those described above, was destined to DUONG's delivery route. Using the  
11 covert cameras in DUONG's delivery vehicle, investigators observed DUONG scan the  
12 parcel, then place it in his backpack, within the delivery vehicle. DUONG then grabbed  
13 his cell phone and exited the vehicle. Using the covert cameras installed in DUONG's  
14 delivery vehicle, investigators observed DUONG throughout his shift. The parcel  
15 appeared to stay within the black backpack. At the end of his shift, DUONG returned to  
16 the Bellevue Carrier Annex and exited the delivery vehicle with his black backpack.  
17 Data from the GPS tracker affixed to DUONG's red Acura showed DUONG drove his  
18 red Acura directly from work to the **SUBJECT PREMISES**.

19 22. On March 17, 2021, investigators conducted surveillance on DUONG with  
20 the assistance of the GPS tracker affixed to DUONG's red Acura. Postal Service records  
21 indicated DUONG was receiving four parcels similar to those described above.  
22 Investigators observed DUONG travel to his residence at 15103 Southeast Newport Way,  
23 Bellevue, Washington, while on duty, after collecting these parcels from the Bellevue  
24 Carrier Annex. In the evening of March 17, 2021, DUONG drove his red Acura to the  
25 **SUBJECT PREMISES**. DUONG knocked on the door and waited. He then turned and  
26 appeared to speak with someone at the door. DUONG then went to DUONG's red Acura  
27 and retrieved what appeared to be a white bag with large square objects in it, which he  
28

1 carried into the residence. DUONG exited the residence shortly after, without the bag or  
2 its contents and departed in his red Acura.

3 23. On March 25, 2021, Postal Service records indicated three Express Mail  
4 parcels, similar to those described above, were destined to DUONG's delivery route.  
5 Using the covert cameras in DUONG's delivery vehicle, investigators observed DUONG  
6 drive his delivery vehicle to his residence at 15103 Southeast Newport Way, Bellevue,  
7 Washington. Duong appeared to carry multiple Express Mail parcels towards the  
8 residence. When DUONG returned to the delivery vehicle, he no longer had the parcels.  
9 Investigators observed DUONG use his Postal Service scanner to scan something on his  
10 cellular phone, multiple times. DUONG then appeared to input information into the  
11 scanner from his cellular phone. These scan times and locations match Postal Service  
12 records for scans associated with the three Express Mail parcels destined to DUONG's  
13 delivery route. Based on my training and experience, I believe DUONG was scanning  
14 images of shipping labels, maintained on his cell phone.

15 24. On March 30, 2021, Postal Service records indicated two Express Mail  
16 parcels, similar to those described above, were destined to DUONG's delivery route.  
17 Using the covert cameras in DUONG's delivery vehicle, investigators observed DUONG  
18 drive his delivery vehicle to his residence at 15103 Southeast Newport Way, Bellevue,  
19 Washington. DUONG exited the delivery vehicle and walked towards the residence.  
20 After returning to the delivery vehicle, DUONG retrieved his wallet and pulled what  
21 appeared to be a credit/debit card from the wallet. DUONG appeared to enter  
22 information from the card into his cell phone. DUONG then used the Postal Service  
23 scanner to scan something on his cell phone and wrote something on the scanner.  
24 Approximately 30 minutes later, DUONG again used the Postal Service scanner to scan  
25 something on his cell phone. These scan times and locations match Postal Service  
26 records for scans associated with the two Express Mail parcels destined to DUONG's  
27 delivery route. Based on my training and experience, I believe DUONG was scanning  
28

1 images of shipping labels, maintained on his cell phone. Data from the GPS affixed to  
2 DUONG's red Acura showed he traveled to the **SUBJECT PREMISES** that evening.

3 25. On April 16, 2021, investigators conducted surveillance on DUONG.  
4 Postal Service records indicated two Express Mail parcels, similar to those described  
5 above, were destined to DOUNG's delivery route and residence. The first was Express  
6 Mail parcel EJ655332919US, which was mailed from Clarksville, TN to the **SUBJECT**  
7 **PREMISES**. Investigators confirmed this parcel was not addressed to DUONG. Earlier,  
8 on April 16, 2021, investigators executed a federal warrant on this parcel and found it to  
9 contain \$83,990.00 in U.S. currency. Investigators placed this mail piece back in the  
10 mail stream after examination. The second parcel was Express Mail parcel  
11 EJ647915820US, which was mailed from Atlanta, GA, to 1660 118th Ave S, Bellevue,  
12 WA 98005. This is a deliverable address on DUONG's delivery route.

13 26. Postal Service records showed both parcels were scanned "Delivered" by  
14 DUONG. Using the covert cameras in DUONG's delivery vehicle, investigators  
15 observed DUONG shove at least one of the Express Mail parcels into his black backpack.  
16 Later, investigators observed DUONG return to the Bellevue Carrier Annex and exit his  
17 delivery vehicle with the backpack. After leaving work, DUONG drove his red ACURA  
18 directly from the Bellevue Carrier Annex to the **SUBJECT PREMISES**. Investigators  
19 observed DUONG enter this residence with the black backpack. Approximately 10  
20 minutes later, investigators observed DUONG exit the residence with the same backpack  
21 and depart in DUONG's red Acura.

22 27. Investigators maintained surveillance on the **SUBJECT PREMISES**. A  
23 blue Chevy Avalanche, bearing Washington license plate C55739M, was parked in front  
24 of the **SUBJECT PREMISES**. Law enforcement records indicated this vehicle was  
25 registered to TAN VAN NGUYEN at 9406 10th Ave Ct E, Tacoma, Washington. At  
26 approximately 90 minutes after DUONG departed the **SUBJECT PREMISES**, a silver  
27 Honda Civic arrived. A young Asian male exited the vehicle, walked up to the front  
28 door, and entered the residence. Shortly after, the same Asian male exited the residence

1 carrying what appeared to be a weighted brown bag. The Asian male entered the silver  
2 Honda Civic and departed. Investigators followed this vehicle to the area near the  
3 Renton airport before losing visual. Law enforcement records showed this vehicle was  
4 registered to TUNG NGUYEN, at 22000 84<sup>th</sup> Avenue South, Trailer 22, Kent,  
5 Washington 98032.

6 28. On April 22, 2021, investigators conducted surveillance on multiple  
7 locations associated to this investigation, including 15103 Southeast Newport Way,  
8 Bellevue, Washington and the **SUBJECT PREMISES**. Postal Service records indicated  
9 two parcels associated with this investigation were destined to DUONG's delivery route.  
10 Postal Service records indicated DUONG drove his delivery vehicle to his residence at  
11 15103 Southeast Newport Way, Bellevue, Washington at approximately 10:13am. Using  
12 the covert cameras in DUONG's delivery vehicle, investigators observed DUONG back  
13 the vehicle up to the residence and exit towards the residence. Based on my prior  
14 experience and observations in this investigation, I believe DUONG took the two Express  
15 Mail parcels from the rear of the delivery vehicle and into the residence.

16 29. At approximately 3:58pm, at 15103 Southeast Newport Way, Bellevue,  
17 Washington, investigators observed an Asian male load something into a blue Toyota  
18 Prius, bearing Washington license plate BKS7412. Law enforcement records showed  
19 this vehicle was registered to DAI TRAN at 15103 Southeast Newport Way, Bellevue,  
20 Washington. After loading something into the trunk of the blue Prius, he departed.  
21 Based on a review of DAI TRAN's driver license photo, the individual observed  
22 appeared to be DAI TRAN.

23 30. At approximately 4:01pm, a white Lexus, bearing Washington license plate  
24 BBC3538 pulled into the driveway at the **SUBJECT PREMISES**. Law enforcement  
25 records showed this vehicle was registered to QUOC PHAM, at 11827 Southeast 189<sup>th</sup>  
26 Place, Renton, Washington. An Asian male exited the vehicle and carried a box to the  
27 front door of the **SUBJECT PREMISES**. He waited for the door to be answered before  
28

1 entering. After approximately seven minutes, the same Asian male exited the **SUBJECT**  
2 **PREMISES**, carrying the same box. He entered the white Lexus and departed.

3 31. At approximately 4:24pm, investigators observed the blue Prius described  
4 above arrive at the **SUBJECT PREMISES**. DAI TRAN carried a box from the vehicle  
5 and waited at the front door. After the door was answered, TRAN carried the box inside.  
6 After approximately eight minutes, DAI TRAN exited the residence, carrying the same  
7 box. He entered the Prius and departed. Investigators observed the Prius arrive at 15103  
8 Southeast Newport Way, Bellevue, Washington at approximately 7:48pm.

9 32. Shortly after the blue Prius departed, the garage door to the **SUBJECT**  
10 **PREMISES** opened and investigators observed an Asian male, an Asian female, and a  
11 small child outside the **SUBJECT PREMISES**. Based on a review of driver license  
12 photos, the Asian male is believed to be TAN VAN NGUYEN. The Asian female is  
13 believed to be TIEN HOANG THAO LE. Two vehicles were parked in the garage. A  
14 Silver Acura MDX, bearing Washington license plate AWW1456, and a black Mercedes,  
15 bearing Washington license plate BLV5332. Law enforcement records showed the silver  
16 Acura was registered to TIEN LE, at 12256 1<sup>st</sup> Avenue Southwest, Seattle, Washington.  
17 Law enforcement records showed the black Mercedes was registered to TAN VAN  
18 NGUYEN, at 9406 10<sup>th</sup> Avenue Court East, Tacoma, Washington. Investigators also  
19 observed a blue Chevy Avalanche parked along the sidewalk in front of the **SUBJECT**  
20 **PREMISES**. Law enforcement records showed the blue Avalanche was registered to  
21 TAN VAN NGUYEN, at 9406 10<sup>th</sup> Avenue Court East, Tacoma, Washington. LE and  
22 NGUYEN appeared to have access and control of the **SUBJECT PREMISES**.  
23 Investigators observed LE, NGUYEN, and the child enter the **SUBJECT PREMISES**  
24 through the open garage. Shortly after, the silver Acura departed and the garage door  
25 closed.

26 33. At approximately 5:40pm, DUONG arrived at 15103 Southeast Newport  
27 Way, Bellevue, Washington, in his red Acura. At approximately 7:50pm, investigators  
28 observed DUONG exit the residence and load what appeared to be a large full black

1 | garbage bag and two boxes, which appeared to be Postal Service boxes, into the rear of  
2 | his red Acura. DAI TRAN brought DUONG a third box from within the residence,  
3 | which DUONG placed inside the rear of the red Acura; before he departed. Investigators  
4 | followed DUONG to a residence located at 2822 South 376<sup>th</sup> Place, Federal Way,  
5 | Washington. DUONG backed up to the residence and appeared to unload items from the  
6 | rear of DUONG's red Acura. After leaving this location, DUONG made a stop in  
7 | Seattle, Washington, before traveling to the **SUBJECT PREMISES**.

### 8 | **TACTICS USED BY DRUG TRAFFICKERS**

9 | 34. Based on my training and experience, and conversations with other  
10 | experienced law enforcement agents and officers who have been involved in narcotics  
11 | cases, I know the following.

12 | 35. The distribution of illegal narcotics is frequently a continuing activity  
13 | lasting over months and years. Persons involved in the trafficking of illegal controlled  
14 | substances typically will obtain and distribute controlled substances on a regular basis,  
15 | much as a distributor of a legal commodity would purchase stock for sale. Similarly,  
16 | such drug traffickers will maintain an "inventory" which will fluctuate in size depending  
17 | upon the demand for and the available supply of the product. Drug traffickers often keep  
18 | records of their illegal activities not only during the period of their drug trafficking  
19 | violations but also for a period of time extending beyond the time during which the  
20 | trafficker actually possesses/controls illegal controlled substances. The records are kept  
21 | in order to maintain contact with criminal associates for future transactions and so that  
22 | the trafficker can have records of prior transactions for which the trafficker might still be  
23 | owed money or might owe someone else money. Dealers often keep these records in  
24 | their homes and in vehicles that they own, use, or have access to.

25 | 36. It is common for drug traffickers to conceal large quantities of U.S.  
26 | currency, foreign currency, cryptocurrency, financial instruments, precious metals,  
27 | jewelry, and other items of value that are proceeds from drug trafficking in their  
28 | residences and in other storage areas associated with the residence, such as on-site

1 storage lockers, garages, detached storage sheds, and parking stalls, or safes located on  
2 the property.

3 37. Evidence of excessive wealth beyond an individual's outward means is  
4 probative evidence of the distribution of controlled substances. Therefore, receipts  
5 showing the expenditure of large sums of money and/or the expensive assets can be  
6 evidence of drug trafficking. Drug traffickers commonly keep the expensive assets  
7 themselves and/or documentation of the purchase of the asset (receipts, warranty cards,  
8 etc.) in their homes, places of business, and in vehicles that they own, use, or have access  
9 to.

10 38. It is common for drug traffickers to maintain equipment and supplies (such  
11 as scales, packaging, and masking agents) on hand over a long period, even when they do  
12 not have any controlled substances on hand. The aforementioned items are frequently  
13 maintained in the drug trafficker's homes, places of business, stash houses, or storage  
14 units, and in vehicles that they own, use, or have access to.

15 39. Drug traffickers often have some amount of inventory—namely, illegal  
16 drugs—stored in their homes, places of business, stash houses or storage units, and in  
17 vehicles that they own, use, or have access to.

18 40. It is common for drug traffickers to possess firearms and ammunition to  
19 protect their drugs, assets, and persons from hostile gangs, rival traffickers, other  
20 criminals, and from law enforcement. Persons who purchase and possess firearms also  
21 tend to maintain the firearms and ammunition for lengthy periods of time. Firearms can  
22 be acquired both legally and unlawfully, without official/traceable documentation.  
23 Persons who acquire firearms from Federal Firearms Licensees, through deliberate fraud  
24 and concealment, often will also acquire firearms from private parties and other sources  
25 unknown to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). Persons  
26 who, whether legally or illegally, purchase, possess, sell and/or transfer firearms or  
27 ammunition commonly maintain the firearms or ammunition on their person, at their  
28 residence or business, or in a motor vehicle which they own and/or operate. Firearms or

1 ammunition are often secreted at other locations within their residential curtilage, and the  
2 identification of these firearms will assist in establishing their origin. Persons who  
3 purchase, possess, sell and/or trade firearms or ammunition commonly maintain  
4 documents and items that are related to the purchase, ownership, possession, sale and/or  
5 transfer of firearms, ammunition, and/or firearm parts, including but not limited to  
6 driver's licenses, telephone records, telephone bills, address and telephone books,  
7 canceled checks, receipts, bank records and other financial documentation on the owner's  
8 person, at the owner's residence or business, or in vehicles that they own, use, or have  
9 access to. Additionally, these individuals often maintain holsters, spare magazines or  
10 speed loaders and other instruments to facilitate the use of firearms in furtherance of  
11 criminal activity or acts of violence.

12 41. It is common for members of drug trafficking organizations, in an attempt  
13 to disguise their identities and illegal activities, to use prepaid cellular telephones and  
14 prepaid long-distance calling cards. Often the only way to connect a subject with a  
15 particular prepaid cellular telephone or calling card is to seize the phone or calling card  
16 from the trafficker or his residence. The aforementioned items are frequently maintained  
17 in the drug trafficker's residence, place of business, or other areas they have access to.

18 42. Drug traffickers often carry many of the items described above—including  
19 (but not limited to) drugs, drug proceeds, firearms, cellular phones—on their person.

20 43. Drug dealers regularly use cell phones and other electronic communication  
21 devices to further their illegal activities. As a result, evidence of drug dealing can often  
22 be found in text messages, address books, call logs, photographs, emails, text messaging  
23 or picture messaging applications, videos, and other data that is stored on cell phones and  
24 other electronic communication devices. Additionally, the storage capacity of such  
25 devices allows them to be used for the electronic maintenance of ledgers, pay/owe logs,  
26 drug weights and amounts, customers contact information, not only during the period of  
27 their drug trafficking violations but also for a period of time extending beyond the time  
28 during which the trafficker actually possesses/controls illegal controlled substances. The

1 records are kept in order to maintain contact with criminal associates for future  
2 transactions and so that the trafficker can have records of prior transactions for which the  
3 trafficker might still be owed money or might owe someone else money.

4 44. Drug traffickers increasingly use applications on smartphones that encrypt  
5 communications such as WhatsApp, or applications that automatically delete messages,  
6 such as Snapchat, in order to avoid law enforcement monitoring or recording of  
7 communications regarding drug trafficking and/or money laundering. Evidence of the  
8 use of such applications can be obtained from smartphones and is evidence of a  
9 smartphone user's efforts to avoid law enforcement detection.

#### 10 **SEARCH AND SEIZURE OF DIGITAL MEDIA**

11 45. As described above and in Attachment B, this application seeks permission  
12 to search for items listed in Attachment B that might be found in **SUBJECT**  
13 **PREMISES**, including digital devices.

14 46. In order to examine digital media in a forensically sound manner, law  
15 enforcement personnel, with appropriate expertise, will conduct a forensic review of any  
16 digital media seized. The purpose of using specially trained computer forensic examiners  
17 to conduct the imaging of any digital media or digital devices is to ensure the integrity of  
18 the evidence and to follow proper, forensically sound, scientific procedures. When the  
19 investigative agent is a trained computer forensic examiner, it is not always necessary to  
20 separate these duties. Computer forensic examiners and investigators often work closely  
21 with investigative personnel to assist investigators in their search for digital evidence.  
22 Computer forensic examiners are needed because they generally have technological  
23 expertise that investigative agents do not possess. Computer forensic examiners,  
24 however, may lack the factual and investigative expertise that an investigate agent may  
25 possess. Therefore, computer forensic examiners and agents often work closely together.  
26 It is intended that the warrant will provide authority for the affiant to forensically review,  
27 or seek the assistance of others in the HSI or within other law enforcement agencies to  
28 assist in the forensic review of any digital devices.

1           47. I also know the following:

2           a. Based my knowledge, training, and experience, I know that  
3 computer files or remnants of such files may be recovered months or even years after  
4 they have been downloaded onto a storage medium, deleted, or viewed via the Internet.  
5 Electronic files downloaded to a storage medium can be stored for years at little or no  
6 cost. Even when files have been deleted, this information can sometimes be recovered  
7 months or years later with forensics tools. This is because when a person “deletes” a file  
8 on a computer, the data contained in the files does not actually disappear; rather, that data  
9 remains on the storage medium until it is overwritten by new data.

10           b. Therefore, deleted files, or remnants of deleted files, may reside in  
11 free space or slack space—that is, in space on the storage medium that is not currently  
12 being used by an active file—for long periods of time before they are overwritten. In  
13 addition, a computer’s operating system may also keep a record of deleted data in “swap”  
14 or “recovery” files.

15           c. Wholly apart from user-generated files, computer storage media—in  
16 particular, computers’ internal hard drives—contain electronic evidence of how a  
17 computer has been used, what it has been used for, and who has used it. To give a few  
18 examples, this forensic evidence can take the form of operating system configurations,  
19 artifacts from operating system or application operation, file system data structures, and  
20 virtual memory “swap” paging files. Computer users typically do not erase or delete this  
21 evidence, because special software is typically required for that task. However, it is  
22 technically possible to delete this information.

23           d. Similarly, files that have been viewed via the Internet are sometimes  
24 automatically downloaded into a temporary Internet directory or “cache.”

25           e. Digital storage devices may also be large in capacity, but small in  
26 physical size. Those who are in possession of such devices also tend to keep them on  
27 their persons, especially when they may contain evidence of a crime. Digital storage  
28

1 devices may be smaller than a postal stamp in size, and thus they may easily be hidden in  
2 a person's pocket.

3 f. As further described in Attachment B, this application seeks  
4 permission to locate not only computer files that might serve as direct evidence of the  
5 crimes described on the warrant, but also for forensic electronic evidence that establishes  
6 how computers were used, the purpose of their use, who used them, and when. There is  
7 probable cause to believe that this forensic electronic evidence will be on digital devices  
8 found in the **SUBJECT PREMISES** because:

9 g. Data on the digital storage medium or digital devices can provide  
10 evidence of a file that was once on the digital storage medium or digital devices but has  
11 since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has  
12 been deleted from a word processing file). Virtual memory paging systems can leave  
13 traces of information on the storage medium that show what tasks and processes were  
14 recently active. Web browsers, e-mail programs, and chat programs store configuration  
15 information on the storage medium that can reveal information such as online nicknames  
16 and passwords. Operating systems can record additional information, such as the  
17 attachment of peripherals, the attachment of USB flash storage devices or other external  
18 storage media, and the times the computer was in use. Computer file systems can record  
19 information about the dates files were created and the sequence in which they were  
20 created, although this information can later be falsified.

21 h. As explained herein, information stored within a computer and other  
22 electronic storage media may provide crucial evidence of the "who, what, why, when,  
23 where, and how" of the criminal conduct under investigation, thus enabling the United  
24 States to further establish and prove each element or alternatively, to exclude the innocent  
25 from further suspicion. In my training and experience, information stored within a  
26 computer or storage media (*e.g.*, registry information, communications, images and  
27 movies, transactional information, records of session times and durations, Internet  
28 history, and anti-virus, spyware, and malware detection programs) can indicate who has

1 used or controlled the computer or storage media. This “user attribution” evidence is  
2 analogous to the search of “indicia of occupancy” while executing a search warrant at a  
3 residence. The existence or absence of anti-virus, spyware, and malware detection  
4 programs may indicate whether the computer was remotely accessed, thus inculcating or  
5 exculpating the computer owner. Further computer and storage media activity can  
6 indicate how and when the computer or storage media was accessed or used. For  
7 example, as described herein, computers typically contain information that log computer  
8 activity associated with user accounts and electronic storage media connected with the  
9 computer. Such information allows investigators to understand the chronological context  
10 of computer or electronic storage media access, use, and events relating to the crime  
11 under investigation. Additionally, some information stored within a computer or  
12 electronic storage media may provide crucial evidence relating to the physical location of  
13 other evidence and the suspect. For example, images stored on a computer may both  
14 show a particular location and have geolocation information incorporated into its file  
15 data. Such file data typically also contains information indicating when the file or image  
16 was created. The existence of such image files, along with external device connection  
17 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
18 camera or cellular phone with an incorporated camera). The geographic and timeline  
19 information described herein may either inculcate or exculpate the computer user.  
20 Lastly, information stored within a computer may provide relevant insight into the  
21 computer user’s state of mind as it relates to the offense under investigation. For  
22 example, information within the computer may indicate the owner’s motive and intent to  
23 commit the crime (e.g., Internet searches indicating criminal planning), or consciousness  
24 of guilt (e.g., running a “wiping” program to destroy evidence on the computer or  
25 password protecting/encrypting such evidence in an effort to conceal it from law  
26 enforcement).

1 i. A person with appropriate familiarity with how a computer works  
2 can, after examining this forensic evidence in its proper content, draw conclusions about  
3 how computers were used, the purpose of their use, who used them, and when.

4 j. The process of identifying the exact files, blocks, registry entries,  
5 logs, or other forms of forensic evidence on a storage medium that are necessary to draw  
6 an accurate conclusion is a dynamic process. While it is possible to specify in advance  
7 the records to be sought, computer evidence is not always data that can be merely  
8 reviewed by a review team and passed along to investigators. Whether data stored on a  
9 computer is evidence may depend on other information stored on the computer and the  
10 application of knowledge about how a computer behaves. Therefore, contextual  
11 information necessary to understand other evidence also falls within the scope of the  
12 warrant.

13 k. Further, in finding evidence of how a computer was used, the  
14 purpose of its use, who used it, and when, sometimes it is necessary to establish that a  
15 particular thing is not present on a storage medium. For example, the presence or  
16 absence of counter-forensic programs or anti-virus programs (and associated data) may  
17 be relevant to establishing a user's intent.

18 l. In most cases, a thorough search of a premises for information that  
19 might be stored on digital storage media or other digital devices often requires the seizure  
20 of the digital devices and digital storage media for later off-site review consistent with the  
21 warrant. In lieu of removing storage media from the premises, it is sometimes possible to  
22 make an image copy of storage media. Generally speaking, imaging is the taking of a  
23 complete electronic copy of the digital media's data, including all hidden sectors and  
24 deleted files. Either seizure or imaging is often necessary to ensure the accuracy and  
25 completeness of data recorded on the storage media, and to prevent the loss of the data  
26 either from accidental or intentional destruction. This is true because of the following:

27 m. *The time required for an examination.* As noted above, not all  
28 evidence takes the form of documents and files that can be easily viewed on site.

1 Analyzing evidence of how a computer has been used, what it has been used for, and who  
2 has used it requires considerable time, and taking that much time on premises could be  
3 unreasonable. As explained above, because the warrant calls for forensic electronic  
4 evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage  
5 media to obtain evidence. Storage media can store a large volume of information.  
6 Reviewing that information for things described in the warrant can take weeks or months,  
7 depending on the volume of data stored, and would be impractical and invasive to  
8 attempt on-site.

9           n.       *Technical requirements.* Computers can be configured in several  
10 different ways, featuring a variety of different operating systems, application software,  
11 and configurations. Therefore, searching them sometimes requires tools or knowledge  
12 that might not be present on the search site. The vast array of computer hardware and  
13 software available makes it difficult to know before a search what tools or knowledge  
14 will be required to analyze the system and its data on-site. However, taking the storage  
15 media off-site and reviewing it in a controlled environment will allow its examination  
16 with the proper tools and knowledge.

17           o.       *Variety of forms of electronic media.* Records sought under this  
18 warrant could be stored in a variety of storage media formats that may require off-site  
19 reviewing with specialized forensic tools.

20       48.       Searching computer systems is a highly technical process that requires  
21 specific expertise and specialized equipment. There are so many types of computer  
22 hardware and software in use today that it is rarely possible to bring to the search site all  
23 the necessary technical manuals and specialized equipment necessary to consult with  
24 computer personnel who have expertise in the type of computer, operating system, or  
25 software application being searched.

26       49.       The analysis of computer systems and storage media often relies on  
27 rigorous procedures designed to maintain the integrity of the evidence and to recover  
28 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-

1 | protected data, while reducing the likelihood of inadvertent or intentional loss or  
2 | modification of data. A controlled environment such as a laboratory, is typically required  
3 | to conduct such an analysis properly.

4 |         50. The volume of data stored on many computer systems and storage devices  
5 | will typically be so large that it will be highly impracticable to search for data during the  
6 | execution of the physical search of the premises. The hard drives commonly included in  
7 | desktop and laptop computers are capable of storing millions of pages of text.

8 |         51. A search of digital devices for evidence described in Attachment B may  
9 | require a range of data analysis techniques. In some cases, agents may recover evidence  
10 | with carefully targeted searches to locate evidence without requirement of a manual  
11 | search through unrelated materials that may be commingled with criminal evidence.  
12 | Agents may be able to execute a “keyword” search that searches through the files stored  
13 | in a digital device for special terms that appear only in the materials covered by the  
14 | warrant. Or, agents may be able to locate the materials covered by looking for a  
15 | particular directory or name. However, in other cases, such techniques may not yield the  
16 | evidence described in the warrant. Individuals may mislabel or hide files and directories;  
17 | encode communications to avoid using keywords; attempt to delete files to evade  
18 | detection; or take other steps designed to hide information from law enforcement  
19 | searches for information.

20 |         52. The search procedure of any digital device seized may include the  
21 | following on-site techniques to seize the evidence authorized in Attachment B:

22 |             a. On-site triage of computer systems to determine what, if any,  
23 | peripheral devices or digital storage units have been connected to such computer systems,  
24 | a preliminary scan of images files contained on such systems and digital storage devices  
25 | to help identify any other relevant evidence or co-conspirators.

26 |             b. On-site copying and analysis of volatile memory, which is usually  
27 | lost if a computer is powered down and may contain information about how the computer  
28 |

1 is being used, by whom, when and may contain information about encryption, virtual  
2 machines, or stenography which will be lost if the computer is powered down.


3 c. On-site forensic imaging of any computers may be necessary for  
4 computers or devices that may be partially or fully encrypted in order to preserve  
5 unencrypted data that may, if not immediately imaged on-scene become encrypted and  
6 accordingly become unavailable for any examination.

7 **CONCLUSION**

8 53. Based on the information set forth herein, there is probable cause to search  
9 the above-described **SUBJECT PREMISES**, as further described in Attachment A, for  
10 evidence, fruits, and instrumentalities, as further described in Attachment B, of crimes  
11 committed by the individual listed in this affidavit and their coconspirators, specifically  
12 distribution of, and possession of, with intent to distribute, controlled substances, in  
13 violation of Title 21, United States Code, Section 841(a)(1).

14  
15  
16   
17 CASEY J. SNYDER  
18 Special Agent  
19 USPS OIG

20 The above-named agent provided a sworn statement to the truth of the foregoing  
21 affidavit by telephone on the 26th day of May, 2021.

22  
23   
24 BRIAN A. TSUCHIDA  
25 United States Magistrate Judge  
26  
27  
28

**ATTACHMENT A****Place to Be Searched (SUBJECT PREMISES)**

The place to be searched is 2000 Northeast 16<sup>th</sup> Street, Renton, Washington 98056, a two-story structure located on the north side of Northeast 16<sup>th</sup> Street and is a corner house. The exterior is a mix of light green/tan siding and rock, with tan trim. The entry door is located to the left of the garage. The numbers “2000” are located to the right side of the garage door.

The search is to include all storage areas associated within the premises, such as on-site storage lockers, detached storage sheds, and parking stalls, or safes; and any digital device(s) or other electronic storage media.



**ATTACHMENT B****List of Items to Be Seized**

Evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Distribution of and Possession with Intent to Distribute Controlled Substances), involving TRI DUONG, as follows:

1. Controlled Substances: Including but not limited to methamphetamine, fentanyl, cocaine, crack cocaine, heroin, hashish, marijuana, MDMA, methadone, oxycodone, Oxycontin, Suboxone, Clonazepam, Alprazolam, Xanax, and Adderall;

2. Drug Paraphernalia: Items used, or to be used, to store, process, package, use, and/or distribute controlled substances, such as plastic bags, DVD cases, cutting agents, scales, measuring equipment, vials, pill presses, Mylar bags, heat/vacuum sealers, tape, duffel bags, chemicals or items used to test the purity and/or quality of controlled substances, and similar items;

3. Drug Transaction Records: Documents such as ledgers, receipts, notes, and similar items relating to the acquisition, transportation, and distribution of controlled substances;

4. Customer and Supplier Information: Items identifying drug customers and drug suppliers, such as telephone records, personal address books, correspondence, diaries, calendars, notes with phone numbers and names, "pay/owe" sheets with drug amounts and prices, maps or directions, and similar items;

5. Cash and Financial Records: Currency and financial records, including bank records, safe deposit box records and keys, credit card records, bills, receipts, tax returns, vehicle documents, and similar items; and other records that show income and expenditures, net worth, money transfers, wire transmittals, negotiable instruments, bank drafts, cashier's checks, and similar items, and money counters;

6. Photographs/Surveillance: Photographs, video tapes, digital cameras, surveillance cameras and associated hardware/storage devices, and similar items, depicting property occupants, friends and relatives of the property occupants, or suspected buyers or sellers of controlled substances, controlled substances or other contraband, weapons, and assets derived from the distribution of controlled substances;

7. Weapons: Including but not limited to firearms, magazines, ammunition, and body armor;

1        8.        Codes: Evidence of codes used in the distribution of controlled substances,  
2 including passwords, code books, cypher or decryption keys, usernames and/or  
3 credentials for dark web marketplaces, and similar information;

4        9.        Property Records: Deeds, contracts, escrow documents, mortgage  
5 documents, rental documents, and other evidence relating to the purchase, ownership,  
6 rental, income, expenses, or control of the premises, and similar records of other property  
7 owned or rented;

8        10.       Indicia of occupancy, residency, and/or ownership of assets including,  
9 utility and telephone bills, canceled envelopes, rental records or payment receipts, leases,  
10 mortgage statements, and other documents;

11       11.       Evidence of Storage Unit Rental or Access: Rental and payment records,  
12 keys and codes, pamphlets, contracts, contact information, directions, passwords or other  
13 documents relating to storage units;

14       12.       Evidence of Personal Property Ownership: Registration information,  
15 ownership documents, or other evidence of ownership of property including, but not  
16 limited to vehicles, vessels, boats, airplanes, jet skis, all-terrain vehicles, RVs, and  
17 personal property; evidence of international or domestic travel, hotel/motel stays, and any  
18 other evidence of unexplained wealth;

19       13.       Individual and business financial books, records, receipts, notes, ledgers,  
20 diaries, journals, and all records relating to income, profit, expenditures, or losses, such  
21 as:

22           a.        Employment records: paychecks or stubs, lists and accounts of  
23 employee payrolls, records of employment tax withholdings and contributions, dividends,  
24 stock certificates, and compensation to officers.

25           b.        Savings accounts: statements, ledger cards, deposit tickets, register  
26 records, wire transfer records, correspondence, and withdrawal slips.

27           c.        Checking accounts: statements, canceled checks, deposit tickets,  
28 credit/debit documents, wire transfer documents, correspondence, and register records.

          d.        Loan Accounts: financial statements and loan applications for all  
loans applied for, notes, loan repayment records, and mortgage loan records.

          e.        Collection accounts: statements and other records.

1 f. Certificates of deposit: applications, purchase documents, and  
2 statements of accounts.

3 g. Credit card accounts: credit cards, monthly statements, and receipts  
4 of use.

5 h. Receipts and records related to gambling wins and losses, or any  
6 other contest winnings.

7 i. Insurance: policies, statements, bills, and claim-related documents.

8 j. Financial records: profit and loss statements, financial statements,  
9 receipts, balance sheets, accounting work papers, any receipts showing purchases made,  
10 both business and personal, receipts showing charitable contributions, and income and  
expense ledgers.

11 14. All bearer bonds, letters of credit, money drafts, money orders, cashier's  
12 checks, travelers checks, Treasury checks, bank checks, passbooks, bank drafts, money  
13 wrappers, stored value cards, and other forms of financial remuneration evidencing the  
14 obtaining, secreting, transfer, and/or concealment of assets and/or expenditures of money;

15 15. All Western Union and/or Money Gram documents and other documents  
16 evidencing domestic or international wire transfers, money orders, official checks,  
17 cashier's checks, or other negotiable interests that can be purchased with cash, to include  
applications, payment records, money orders, frequent customer cards, etc;

18 16. Negotiable instruments, jewelry, precious metals, financial instruments, and  
19 other negotiable instruments;

20 17. Documents reflecting the source, receipt, transfer, control, ownership, and  
21 disposition of United States and/or foreign currency;

22 18. Correspondence, papers, records, and any other items showing employment  
23 or lack of employment;

24 19. Telephone books, and/or address books, facsimile machines, any papers  
25 reflecting names, addresses, telephone numbers, pager numbers, cellular telephone  
26 numbers, facsimile, and/or telex numbers, telephone records and bills relating to co-  
27 conspirators, sources of supply, customers, financial institutions, and other individuals or  
28 businesses with whom a financial relationship exists. Also, telephone answering devices  
that record telephone conversations and the tapes therein for messages left for or by co-

1 conspirators for the delivery or purchase of controlled substances or laundering of drug  
2 proceeds;

3 20. Safes and locked storage containers, and the contents thereof which are  
4 otherwise described in this document;

5 21. Tools: Tools that may be used to open hidden compartments in vehicles,  
6 paint, bonding agents, magnets, or other items that may be used to open/close said  
7 compartments;

8 22. Any and all mailing documents and packaging materials related to U.S.  
9 Postal Service, UPS, and FedEx, including but not limited to USPS Express Mail labels,  
10 express mail and priority envelopes, first class mailings, receipts for USPS packages, and  
11 tracking information;

12 23. Any records or information pertaining to the dark web and dark web  
13 marketplaces, including the Empire Market, Deep Sea Market, and White House Market;

14 24. Any records or information pertaining to darknet monikers;

15 25. Cryptocurrency applications and wallets, including information regarding  
16 current account balance and transaction history, i.e., date, time, amount, an address of the  
17 sender/recipient of a cryptocurrency transaction maintained in such wallets;

18 26. Any records or information reflecting cryptocurrencies, including web  
19 history, and documents showing the location, source, and timing of acquisition of any  
20 cryptocurrencies, including wallets, wallet addresses, and seed phrases;

21 27. Any and all cryptocurrency, to include the following: (a) any and all  
22 representations of cryptocurrency public keys or addresses, whether in electronic or  
23 physical format; (b) any and all representations of cryptocurrency private keys, whether  
24 in electronic or physical format; and (c) any and all representations of cryptocurrency  
25 wallets or their constitutive parts, whether in electronic or physical format, to include  
26 "recovery seeds" and "root keys" which may be used to regenerate a wallet.

27 a. The United States is authorized to seize any and all cryptocurrency  
28 by transferring the full account balance in each wallet to a public cryptocurrency address  
controlled by the United States.

1           b.     The United States is also authorized to use the above-described  
2 recovery seeds and root keys to reconstitute and/or regenerate any associated  
3 cryptocurrency wallet and to seize any and all cryptocurrency stored in, or accessible via,  
4 such wallet by transferring the full account balance to a public cryptocurrency address  
5 controlled by the United States.

6           28.    Cell Phones: Cellular telephones and other communications devices may be  
7 seized, and searched for the following items:

8           a.     Assigned number and identifying telephone serial number (ESN,  
9 MIN, IMSI, or IMEI);

10           b.    Stored list of recent received, sent, and missed calls;

11           c.    Stored contact information;

12           d.    Stored photographs of narcotics, currency, firearms or other  
13 weapons, evidence of suspected criminal activity, and/or the user of the phone and/or co-  
14 conspirators, including any embedded GPS data associated with these photographs;

15           e.    Stored text messages, as well as any messages in any internet  
16 messaging apps, including but not limited to Facebook Messenger, iMessage, Wickr,  
17 Telegram, Signal, WhatsApp, Kik, and similar messaging applications, related to the  
18 aforementioned crimes of investigation or that may show the user of the phone and/or  
19 co-conspirators, including Apple iMessages, Blackberry Messenger messages or other  
20 similar messaging services where the data is stored on the telephone;

21           f.    Any Tor applications and records for Tor activity, including browser  
22 history and “bookmarked” or “favorite” web pages;

23           g.    Digital currency applications and wallets, to include information  
24 regarding current account balance and transaction history, i.e., date, time, amount, an  
25 address of the sender/recipient of a digital currency transaction maintained in such  
26 wallets;

27           h.    Stored documents, notes, and files that contain passwords/or  
28 encryption keys;

          i.    PGP applications, to include stored private and/or public keys;

          j.    Any records or information related to darknet monikers; and

1        29. Digital devices, such as computers, and other electronic storage media,  
2 such as USBs and Trezor devices, may be seized, and searched for the following items:

3            a. Evidence of who used, owned, or controlled the digital device or  
4 other electronic storage media at the time the things described in this warrant were  
5 created, edited, deleted, such as logs, registry entries, configuration files, saved  
6 usernames and passwords, documents, browsing history, user profiles, email, email  
7 contacts, "chats," instant messaging logs, photographs, and correspondence;

8            b. Evidence of software that would allow others to control the digital  
9 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
10 of malicious software, as well as evidence of the presence or absence of security software  
11 designed to detect malicious software;

12            c. Evidence of the lack of such malicious software;

13            d. Evidence of the attachment to the digital device of other storage  
14 devices or similar containers for electronic evidence;

15            e. Evidence of counter-forensic programs (and associated data) that are  
16 designed to eliminate data from the digital device or other electronic storage media;

17            f. Evidence of the times the digital device or other electronic storage  
18 media was used;

19            g. Passwords, encryption keys, and other access devices that may be  
20 necessary to access the digital device or other electronic storage media;

21            h. Contextual information necessary to understand the evidence  
22 described in this attachment;

23            i. Records or information pertaining to the dark web and dark web  
24 marketplaces, including the Empire Market;

25            j. Any records or information pertaining to darknet monikers;

26            k. Any records or information pertaining to Tor;

27            l. Any records or information pertaining to mnemonic phrases;

1           m. Any records or information reflecting cryptocurrencies, including  
2 web history, and documents showing the location, source, and timing of acquisition of  
3 any cryptocurrencies, to include wallets, wallet addresses, and seed phrases; and

4           n. Any records or information pertaining to PGP applications, to  
5 include private and/or public keys.

6 THE SEIZURE OF DIGITAL DEVICES IS AUTHORIZED FOR THE PURPOSE OF  
7 CONDUCTING OFF-SITE EXAMINATION OF THEIR CONTENTS FOR  
8 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
9 CRIMES.  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28